

JUN 14 2006

Attorney's Docket No. 9407-40 (GB920010095US1)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: John Owlett

Serial No.: 10/081,500

Filed: February 22, 2002

For: METHOD AND SYSTEM FOR AUTHENTICATION OF A USER

Confirmation No.: 1505

Group No.: 2131

Examiner: Christian A. LaForgia

June 14, 2006

Mail Stop Appeal-Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being transmitted
by facsimile to the U.S. Patent and Trademark Office via
facsimile number 571-273-8300 on June 14, 2006

Michele P. McMahan
Michele P. McMahan

**TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION—37 C.F.R. § 41.37)**

1. Transmitted herewith is the APPEAL BRIEF for the above-identified application, pursuant to the Notice of Appeal filed on April 24, 2006.

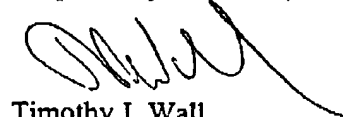
2. This application is filed on behalf of
☐ a small entity.

3. Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:
☐ small entity \$250.00
☒ other than small entity \$500.00

Appeal Brief fee due \$500.00

☒ You may charge Deposit Account 09-0657 for the Appeal Brief and any additional charges or deficiency in funds.

Respectfully submitted,



Timothy J. Wall

Registration No. 50,743

**RECEIVED
CENTRAL FAX CENTER****JUN 14 2006**

MYERS BIGEL SIBLEY & SAJOVEC, P.A.
Patent Attorneys
4140 Parklake Avenue, Suite 600, Raleigh, NC 27612
or
P.O. Box 37428
Raleigh, NC 27627
919-854-1400
Facsimile 919-854-1401

**TELECOPIER TRANSMISSION
COVER SHEET**

Date: June 14, 2006 **File Number:** 9407-40

Telecopier No.: 571-273-8300 **Telephone No.:**

To: Commissioner for Patents

Company: U.S. Patent and Trademark Office

From: Timothy J. Wall

Number of Pages: 19 **Return fax to:** Michele

If there is a problem with this transmission, please call (919) 854-1400. Our fax number is (919) 854-1401.

In re: John Owlett
Serial No. 10/081,500
Filed: February 22, 2002
Confirmation No. 1505

Enclosed is an Appeal Brief in the above-referenced application.

Confidentiality Note

The information contained in this facsimile message is legally privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby prohibited. If you have received this telecopy in error, please immediately notify us by telephone and return the original message to us at the address above via the United States Postal Service. **THANK YOU.**

JUN 14 2006

Attorney's Docket No. 9407-40 (GB920010095US1)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: John Owlett

Confirmation No.: 1505

Serial No.: 10/081,500

Group No.: 2131

Filed: February 22, 2002

Examiner: Christian A. LaForgia

For: METHOD AND SYSTEM FOR AUTHENTICATION OF A USER

Mail Stop Appeal-Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being transmitted
by facsimile to the U.S. Patent and Trademark Office via
facsimile number 571-273-8300 on June 14, 2006

Michele P. McMahan
Michele P. McMahan

APPELLANT'S BRIEF ON APPEAL UNDER 37 C.F.R. §41.37

Sir:

This Appeal Brief is filed pursuant to the "Notice of Appeal to the Board of Patent Appeals and Interferences" mailed April 24, 2006.

Real Party In Interest

The real party in interest is assignee International Business Machines Corporation, Armonk, New York.

Related Appeals and Interferences

Appellant is aware of no appeals or interferences that would be affected by the present appeal.

Status of Claims

Appellant appeals the final rejection of Claims 1-14, which as of the filing date of this Brief remain under consideration. The attached Appendix A presents the claims at issue as finally rejected in the Final Office Action of January 24, 2006 (hereinafter "Final Office Action") and the Advisory Action of April 12, 2006 (hereinafter "Advisory Action").

06/27/2006 MAHMED1 00000013 090457 10081500

01 FC:1402 500.00 DA

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 2 of 17

Status of Amendments

The attached Appendix A presents the pending claims and each of the pending claims corresponding status. All amendments in the present case have been entered.

Summary of the Claimed Subject Matter

The present application includes Independent Claims 1, 13, and 14. The claims are method, system and computer program product claims. Claim 1 is directed to methods for authentication of a user by an authenticating entity. Such methods may be provided by the authenticating entity sending a challenge to a user. *See Specification, page 10, lines 14-16 and Figure 3 (block 310).* The user adds a spoiler to the challenge. *See Specification, page 10, lines 17-19 and Figure 3 (block 314).* The user encrypts the combined spoiler and challenge using a private key of an asymmetric key pair. *See Specification, page 10, lines 19-22 and Figure 3 (block 316).* The user sends a response to the authenticating entity in the form of the encrypted combined spoiler and challenge. *See Specification, page 10, lines 23-24 and Figure 3 (block 318).*

Independent Claim 13 is directed to a system for authentication of a user. The system includes a first application and an authenticating second application. Structure corresponding to the means recitations found in Claim 13 is provided, inter alia, by a processor for carrying out the functions of instructions loaded into a system. *See Specification, page 14, lines 5-8 and Figures 3 and 4.* Thus, structure corresponding to the "the authenticating second application having means for sending a challenge to the first application" is provided, inter alia, by a processor, for example the processor used to perform the function of block 310 of Figure 3. *See Specification, page 10, lines 14-16 and Figure 3 (block 310).* Structure corresponding to the "the first application having means for adding a spoiler to the challenge and means for encrypting the combined spoiler and challenge with a private key of an asymmetric key pair" is provided, inter alia, by a processor, for example the processor used to perform the function of blocks 314 and 316 of Figure 3. *See Specification, page 10, lines 17-22 and Figure 3 (blocks 314 and 316).* Structure corresponding to the "means for sending the encrypted combined spoiler and challenge from the first application to the authenticating second application" is provided, inter alia, by a processor, for example the processor used to perform the function of block 318 of Figure 3. *See Specification, page 10, lines 23-24 and Figure 3 (block 318).*

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 3 of 17

Independent Claim 14 is directed to a computer program product corresponding to Claim 1.

Claim 2 is directed to aspects of the invention where the authenticating entity decrypts the encrypted combined spoiler and challenge using the public key of the asymmetric key pair and determines if the user has been authenticated. *See* Specification, page 10, lines 28-30 and Figure 3 (block 322).

Claim 3 is directed to aspects of the invention where the spoiler is added by applying a spoiler function to the challenge. *See* Specification, page 11, lines 24-27 and Figure 4 (block 414).

Claim 4 is directed to aspects of the invention that send the form of the spoiler function to the authenticating entity. *See* Specification, page 12, lines 1-5 and Figure 4 (block 420).

Claim 5 is directed to aspects of the invention where the spoiler is added to the challenge as a prefix or a suffix and the authenticating entity extracts the challenge by counting the number of bytes from the beginning or end of the combined spoiler and challenge. *See* Specification, page 11, lines 7-13 and Figure 3 (block 326).

Claim 6 is directed to aspects of the invention where the user obtains a digest of the combined spoiler and challenge before the step of encrypting. *See* Specification, page 11, lines 24-27 and Figure 4 (block 416).

Claim 7 is directed to aspects of the invention where the user obtains the digest by applying a hash function to the combined spoiler and challenge. *See* Specification, page 11, lines 24-27 and Figure 4 (block 416).

Claim 8 is directed to aspects of the invention where the user sends details of the spoiler and the method of obtaining the digest to the authenticating entity. *See* Specification, page 12, lines 1-5 and Figure 4 (block 420).

Claim 9 is directed to aspects of the invention where the user sends details of the algorithm used for encryption to the authenticating entity. *See* Specification, page 12, lines 1-5 and Figure 4 (block 422).

Claim 10 is directed to aspects of the invention where the authenticating entity obtains a digest of the combined spoiler and the original challenge that the authenticating entity sent to the user and compares the digest to a digest obtained by decrypting the response from the user. *See* Specification, page 12, lines 5-20 and Figure 4 (blocks 414, 430, and 432).

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 4 of 17

Claim 11 is directed to aspects of the invention where the challenge is a bit sequence. *See* Specification, page 10, lines 13-14 and Figure 3 (block 310).

Claim 12 is directed to aspects of the invention where the spoiler is an additional bit sequence. *See* Specification, page 11, lines 7-13 and Figure 3 (block 314).

Grounds of Rejection to Be Reviewed on Appeal

1. Claims 1-5 and 11-14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over United States Application Publication No. 2002/0034301 to Andersson (hereinafter "Andersson") in view of United States Application Publication No. 2004/0202328 to Hara (hereinafter "Hara").

2. Claims 6-8 and 10 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Andersson in view of Hara, and further in view of United States Patent No. 6,072,875 to Tsudik (hereinafter "Tsudik").

Argument

I. Introduction

The pending claims are rejected as obvious under 35 U.S.C. § 103. To establish a *prima facie* case of obviousness, the prior art reference or references when combined must teach or suggest *all* the recitations of the claims, and there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. M.P.E.P. §2143. The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. M.P.E.P. §2143.01, citing *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990). As emphasized by the Court of Appeals for the Federal Circuit, to support combining references, evidence of a suggestion, teaching, or motivation to combine must be **clear and particular**, and this requirement for clear and particular evidence is not met by broad and conclusory statements about the teachings of references. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). The Court of Appeals for the Federal Circuit has further stated that, to support combining or modifying references, there must be **particular** evidence from the prior art as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000).

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 5 of 17

Appellant respectfully submits that the pending claims are patentable over the cited references because the cited references fail to disclose or suggest the recitations of the pending claims.

II. The Section 103 Rejection

A. The Rejection of Independent Claims 1, 13 and 14

As stated above, Independent Claims 1, 13 and 14 stand rejected under 35 U.S.C. § 103 as being unpatentable over Andersson in view of Hara. Appellant respectfully submits that many of the recitations of these claims are neither disclosed nor suggested by the cited references. For example, Claim 1 recites:

A method for authentication of a user by an authenticating entity comprising the steps of:
the authenticating entity sending a challenge to the user;
the user adding a spoiler to the challenge;
the user encrypting the combined spoiler and challenge using a private key of an asymmetric key pair;
the user sending a response to the authenticating entity in the form of the encrypted combined spoiler and challenge.

Claims 13 and 14 contain corresponding system and computer program product claims, respectively. Appellant submits that at least the highlighted portions of, for example, Claim 1, are neither disclosed nor suggested by Andersson in view of Hara.

The Final Office Action states that Andersson teaches all the recitations of Claim 1 except for "adding a spoiler to the challenge and encrypting the combined spoiler and challenge." *See* Final Office Action, page 4. However, the Final Office Action points to Hara as providing the missing teachings. *See* Final Office Action, page 4. Appellant respectfully disagrees. In particular, the cited portion of Andersson discusses a conventional encryption system that includes sending a challenge to the requesting party. *See* Andersson, page 3, paragraph 40. In fact, this type of conventional encryption system is discussed in the Background of the present application. *See* Figure 2 and corresponding text. Appellant does not dispute that the use of a challenge as discussed in Andersson is known. However, Claim 1 recites **"adding a spoiler to the challenge; encrypting the combined spoiler and challenge using a private key of an asymmetric key pair and sending a response to the authenticating entity in the form of the encrypted combined spoiler and challenge."** Nothing in

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 6 of 17

Andersson discloses or suggests at least these recitations of Claim 1. Furthermore, Hara does not provide the missing teachings.

In particular, the cited portion of Hara states:

[0083] As shown in FIG. 7B, the data transmitter 2 performs data encapsulation in accordance with the first protocol first by padding the IP datagram (i.e., adding a padding part 102) to make the length of the data part an integer multiple of 64 bits. For example, a padding part of 0 to 63 bits is suffixed to the IP datagram 101. All bits in the padding part are "1" each. The padding is intended to keep the datagram to a predetermined data length because the data part is better suited for encryption when its length is an integer multiple of 64 bits. The data part placed in the format of the first protocol is called a section hereunder.

[0084] The section supplemented with the padding 102 is then encrypted by the data transmitter 2 as shown in FIG. 7C. Encryption is carried out by use of encryption keys. The encryption keys are session keys (described later) used to encrypt information to be sent to the data receiver 3. The encryption method adopted here is a block encryption method based on the common key cryptosystem such as the Triple-DES. The Triple-DES encryption is one of today's strongest public key cryptosystems and is easy to implement for high-speed encryption on a hardware basis. This encryption process, unlike that of most public key cryptosystems, is fast enough to keep up with transmission at rates of as high as 30 Mbps.

See Hara, paragraphs 83 and 84 (emphasis added). The cited portion of Hara discusses filling in bits in an IP datagram with "1's" so as to create a 64 bit datagram, which is better suited for encryption. Thus, Hara basically discusses adding place holders in the IP datagram. Nothing in Hara discusses the addition of a "spoiler" as recited in Claim 1. In fact, the addition of 1's discussed in Hara would not provide any added level of security as a "spoiler" that is always all 1's is easy to figure out. Accordingly, Hara does not provide the missing teachings.

In response to Appellant's arguments presented above, the Final Office Action states:

The Appellant defines a spoiler in page 8 of the specification as "be[ing] added to the challenge as a prefix or a suffix and the authenticating entity extracts the challenge by counting the number of bytes from the beginning or end of the combined spoiler and challenge." Hara discloses adding padding to data and then encrypting the data along with padding the data, because the data is then better suited for encryption (see paragraphs [0083] and [0084]).

See Final Office Action, page 2. First, the cited portion of Appellant's specification is not the definition of a spoiler as used therein. The cited portion of Appellant's specification is found in the Summary of the Invention, and discusses features of some embodiments of the present invention. The spoiler according to some embodiments of the present invention is added to a challenge to enhance the authentication of a user, thus, providing more security to the users

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 7 of 17

of the system. Appellant does not see how "adding padding to data", *i.e.* adding a bunch of 1's to the IP datagram, to create a 64 bit datagram, which is easier to encrypt, teaches a spoiler as recited in the claims of the present application. Nothing in Appellant's specification even suggests the addition of bits simply to normalize the encryption process. In fact, as discussed above, the addition of 1's discussed in Hara would not provide the added level of security provided by a "spoiler" according to some embodiments of the present invention, as the padding is always all 1's and, therefore, easy to figure out. Accordingly, Appellant submits that the cited combination does not teach adding a spoiler to the challenge as recited in the claims of the present invention for at least these additional reasons.

In addition to the reasons set forth above for reversing the obviousness rejections, there is also no proper motivation to combine the cited references in the manner suggested in the Final Office Action. Responsive to Appellant's arguments in their Amendment of March 15, 2004, the Final Office Action cites *In re MacLaughlin*, which is a Court of Customs and Patent Appeals case from 1971. More recent case law of the Court of Appeals for the Federal Circuit makes clear that this does not imply that sweeping, conclusory inferences drawn from multiple references meet the requirements for support of a rejection under § 103. In particular, to support combining references, evidence of a suggestion, teaching, or motivation to combine must be *clear and particular*, and this requirement for clear and particular evidence is not met by broad and conclusory statements about the teachings of references. *See, e.g., In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). The Final Office Action does not point to any portion of the cited references as providing a motivation to combine the references. Each of the cited references include different uses of challenges, padding bits, and the like, and a § 103 rejection may not be supported simply by throwing these disparate arrangements of teachings together in an *ad hoc* fashion, as these proposed changes would fundamentally change the functionalities of the inventions described in the cited references. For example, the Final Office Action combines three references to allegedly teach the recitations of Claims 6-8 and 10. The more references that need to be combined to allegedly teach the recitations of particular claims, the less obvious the combination becomes. A person of skill in the art would not be motivated to combine these references without using Appellant's disclosure as a road map. Thus, it appears that the Final Office Action gains its impetus or suggestion to modify the cited reference by hindsight reasoning informed by

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 8 of 17

Appellant's disclosure, which, as noted above, is an inappropriate basis for combining references.

Responsive to Appellant's arguments that there is no suggestion to combine the references, the Final Office Action states:

In this case, the references provide a teaching, suggestion and motivation for combining the references. As disclose in Hara, in particular paragraph [0084], adding padding makes the data to be encrypted better suited for encryption.

See Final Office Action, pages 2-3. As discussed above, the "spoiler" as recited in the claims of the present application does not just "pad" the data to simplify the encryption process. Accordingly, this teaching of Hara would not provide a motivation to combine the references as suggested in the Final Office Action. Furthermore, the Final Office Action misinterprets the cited portion of Hara. Nothing in the cited portion of Hara states that the padding makes the encryption "stronger", only that a length of 64 bits is "better suited" for encryption, *i.e.*, easier to encrypt as it is a more standard length. Again, as discussed above, adding all 1's is not going to strengthen the encryption as much as "spoiler", as it would be easy to predict. Furthermore, even if Andersson and Hara could be properly combined, the combination of Andersson and Hara would not teach the recitations of the pending claims for at least the reasons discussed above.

The Final Office Action further misinterprets Appellant's arguments as the Final Office Action states that Appellant argued that "the question of motivation to add padding is based on subjective belief and unknown authority." See Final Office Action, page 3. In fact, Appellant's argument is that the motivation to combine the references is not found within the references themselves or the art and, thus, the motivation to combine must be found in Appellant's disclosure, which is improper. Furthermore, even if the teaching of padding found in Hara were combined with the teachings of Andersson, the combination does not teach the recitations of the claims of the present application.

Finally, the Final Office Action states that "it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based on hindsight reasoning." See Final Office Action, page 3. Appellant agrees. However, as affirmed by the Court of Appeals for the Federal Circuit in *In re Sang-su Lee* in a much more recent decision, "[i]t is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to [use] that which the inventor taught against its teacher."

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 9 of 17

Thus, the motivation must come from outside the four corners of the application. The Office must point to some teaching in the art or cited references that would motivate a person of skill to combine the references as suggested. The Final Office Action does not point to such a teaching. In particular, Andersson discusses network authentication that uses a conventional challenge responsive to a request. *See* Andersson, page 3, paragraph 40. Hara, on the other hand, discusses a data transmission method including encryption where the header is padded with 1's to create a 64 bit block that may be well suited for encryption. *See* Hara, paragraphs 83 and 84. A skilled artisan would not be motivated to combine these references without using the teachings of Appellant's disclosure as a guide.

Accordingly, Appellant respectfully submits that Independent Claims 1, 13 and 14 are patentable over the cited combination for at least these additional reasons. Furthermore, the dependent claims are patentable at least per the patentability of independent Claim 1 from which they depend. Accordingly, Appellant submits that independent Claims 1, 13 and 14 and the claims that depend therefrom are in condition for allowance, which is respectfully requested in due course. For at least these reasons, Appellant requests that the rejection of Claims 1-14 be reversed.

B. Many of the Dependent Claims are Separately Patentable

As stated above, Claims 2-5 and 11-12 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Andersson in view of Hara. Many of the dependent claims are separately patentable over the cited combination.

1. Claim 2 is Separately Patentable

For example, Claim 2 recites:

A method as claimed in claim 1, wherein the method includes the authenticating entity decrypting the encrypted combined spoiler and challenge using the public key of the asymmetric key pair and determining if the user has been authenticated.

As discussed above, nothing in Andersson or Hara discloses or suggests a combined spoiler and challenge as recited in the claims of the present application. Accordingly, it follows that nothing in the cited references discloses or suggests encryption of the combined spoiler and challenge as recited in Claim 2. Accordingly, Claim 2 is separately patentable over the cited references for at least these additional reasons. For at least these reasons, Appellant requests that the rejection of Claim 2 be reversed.

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 10 of 17

2. Claims 3-5 are Separately Patentable

Claims 3 through 5 recite details of the spoiler. As discussed above, nothing in the cited references discloses or suggests a spoiler as recited in the claims of the present application. Accordingly, it follows that nothing in the cited references discloses or suggests details with respect to the spoiler as recited in Claims 3-5. Accordingly, Claims 3-5 are separately patentable over the cited references for at least these additional reasons. For at least these reasons, Appellant requests that the rejection of Claims 3-5 be reversed.

3. Claims 6-8 and 10 are Separately Patentable

As stated above, Claims 6-8 and 10 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Andersson in view of Hara, and further in view of Tsudik.

The Final Office Action admits that the combination of Andersson and Hara do not disclose or suggest the recitations of Claims 6-8 and 10. *See* Final Office Action, page 6. However, the Final Office Action points to Tsudik as providing the missing teachings. *See* Final Office Action, pages 6-7. Appellant respectfully disagrees. Claims 6-8 and 10 contain details of obtaining a digest according to some embodiments of the present invention. In particular, Claim 6 recites "obtaining a digest of the combined spoiler and challenge before the step of encrypting." The cited portion of Tsudik states:

Communication between mobile users of and in a computer network is subject to a variety of security issues; user identification and user tracking are two particularly important ones. This invention provides a method and an apparatus for securely identifying a mobile user while avoiding trackability of his/her movements, i.e. it provides a way for a secure user identification in secrecy. The gist is to encrypt the user's identifier, and/or his/her password, and a synchronization indication, preferably a fixed time interval, under a secret one-way function and sending the encrypted message, herein called "dynamic user identifier", to the user's "home authority" where he/she is registered. The home authority comprises correspondence tables listing, pre-computed for every time interval (or another chosen synchronization), the dynamic user identifiers and the corresponding true identity of the user and can thus quickly decide whether the received encrypted message originates from a registered user. On the other hand, an intruder is neither able to detect from the encrypted messages the identity of the user nor can he/she track a user's moves.

See Tsudik, column 3, line 59 to column 4, line 11. Nothing in the cited portion of Tsudik discloses or suggests the digest recitations of Claims 6-8 and 10. Accordingly, Claims 6-8 and 10 are separately patentable over the cited combination for at least these additional

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 11 of 17

reasons. For at least these reasons, Appellant requests that the rejection of Claims 6-8 and 10 be reversed.

4. Claim 9 is Separately Patentable

Although the Final Office Action does not specifically reject claim 9 under 35 U.S.C. § 103(a), the Final Office Action does state that "Tsudik teaches wherein the user sends details of the algorithm used for encryption to the authenticating entity (column 5, lines 27-48)." *See* Final Office Action, p. 7. The Final Office Action further states that "[i]t would have been obvious to one of ordinary skill in the art at the time of the invention was made to send details of the encryption to be used by mobile users, since Tsudik states at column 4, lines 12-21 that such modification would allow for mobile users while minimizing the traceability and possibility of identifying the mobile user." *See* Final Office Action, page 7. Appellant respectfully disagrees. Claim 9 recites "wherein the user sends details of the algorithm used for encryption to the authenticating entity." The cited portions of Tsudik do not disclose or suggest the algorithm recitations of Claim 9. Accordingly, Claim 9 is separately patentable over the cited combination for at least these additional reasons. For at least these reasons, Appellant requests that the apparent rejection of Claim 9 be reversed.

For at least the foregoing reasons, Appellant respectfully submits that many of the dependent claims are also separately patentable over the cited references. Accordingly, Appellant respectfully requests reversal of the rejections with respect to the dependent claims for at least these additional reasons.

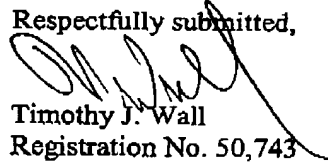
In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 12 of 17

III. Conclusion

In light of the above, Appellant requests reversal of the rejections of the claims, allowance of the claims and passing of the application to issue.

It is not believed that an extension of time and/or additional fee(s) are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned for under 37 C.F.R. §1.136(a). Any additional fees believed to be due in connection with this paper may be charged to Deposit Account No. 09-0657.

Respectfully submitted,



Timothy J. Wall
Registration No. 50,743

Customer No. 46590
Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 13 of 17

APPENDIX A

1. (Original) A method for authentication of a user by an authenticating entity comprising the steps of:
 - the authenticating entity sending a challenge to the user;
 - the user adding a spoiler to the challenge;
 - the user encrypting the combined spoiler and challenge using a private key of an asymmetric key pair;
 - the user sending a response to the authenticating entity in the form of the encrypted combined spoiler and challenge.
2. (Original) A method as claimed in claim 1, wherein the method includes the authenticating entity decrypting the encrypted combined spoiler and challenge using the public key of the asymmetric key pair and determining if the user has been authenticated.
3. (Original) A method as claimed in claim 1, wherein the addition of a spoiler to the challenge is carried out by applying a spoiler function to the challenge.
4. (Original) A method as claimed in claim 3, wherein the form of the spoiler function is sent to the authenticating entity.
5. (Original) A method as claimed in claim 1, wherein the spoiler is added to the challenge as a prefix or a suffix and the authenticating entity extracts the challenge by counting the number of bytes from the beginning or end of the combined spoiler and challenge.
6. (Original) A method as claimed in claim 1, wherein the method includes the user obtaining a digest of the combined spoiler and challenge before the step of encrypting.
7. (Original) A method as claimed in claim 6, wherein the user obtains the digest by applying a hash function to the combined spoiler and challenge.

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 14

8. (Original) A method as claimed in claim 6, wherein the user sends details of the spoiler and the method of obtaining the digest to the authenticating entity.

9. (Original) A method as claimed in claim 1, wherein the user sends details of the algorithm used for encryption to the authenticating entity.

10. (Original) A method as claimed in claim 8, wherein the authenticating entity obtains a digest of the combined spoiler and the original challenge that the authenticating entity sent to the user and compares the digest to a digest obtained by decrypting the response from the user.

11. (Original) A method as claimed in claim 1, wherein the challenge is a bit sequence.

12. (Original) A method as claimed in claim 1, wherein the spoiler is an additional bit sequence.

13. (Original) A system for authentication of a user comprising a first application and an authenticating second application,
the authenticating second application having means for sending a challenge to the first application,
the first application having means for adding a spoiler to the challenge and means for encrypting the combined spoiler and challenge with a private key of an asymmetric key pair,
and
means for sending the encrypted combined spoiler and challenge from the first application to the authenticating second application.

14. (Original) A computer program product stored on a computer readable storage medium for authentication of a user by an authenticating entity, comprising computer readable program code means for performing the steps of:
the authenticating entity sending a challenge to the user;

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 15

the user adding a spoiler to the challenge;
the user encrypting the combined spoiler and challenge using a private key of an asymmetric key pair;
the user sending a response to the authenticating entity in the form of the encrypted combined spoiler and challenge.

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 16

APPENDIX B – EVIDENCE APPENDIX
(NONE)

In re: John Owlett
Serial No.: 10/081,500
Filed: February 22, 2002
Page 17

**APPENDIX C – RELATED PROCEEDINGS
(NONE)**

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.